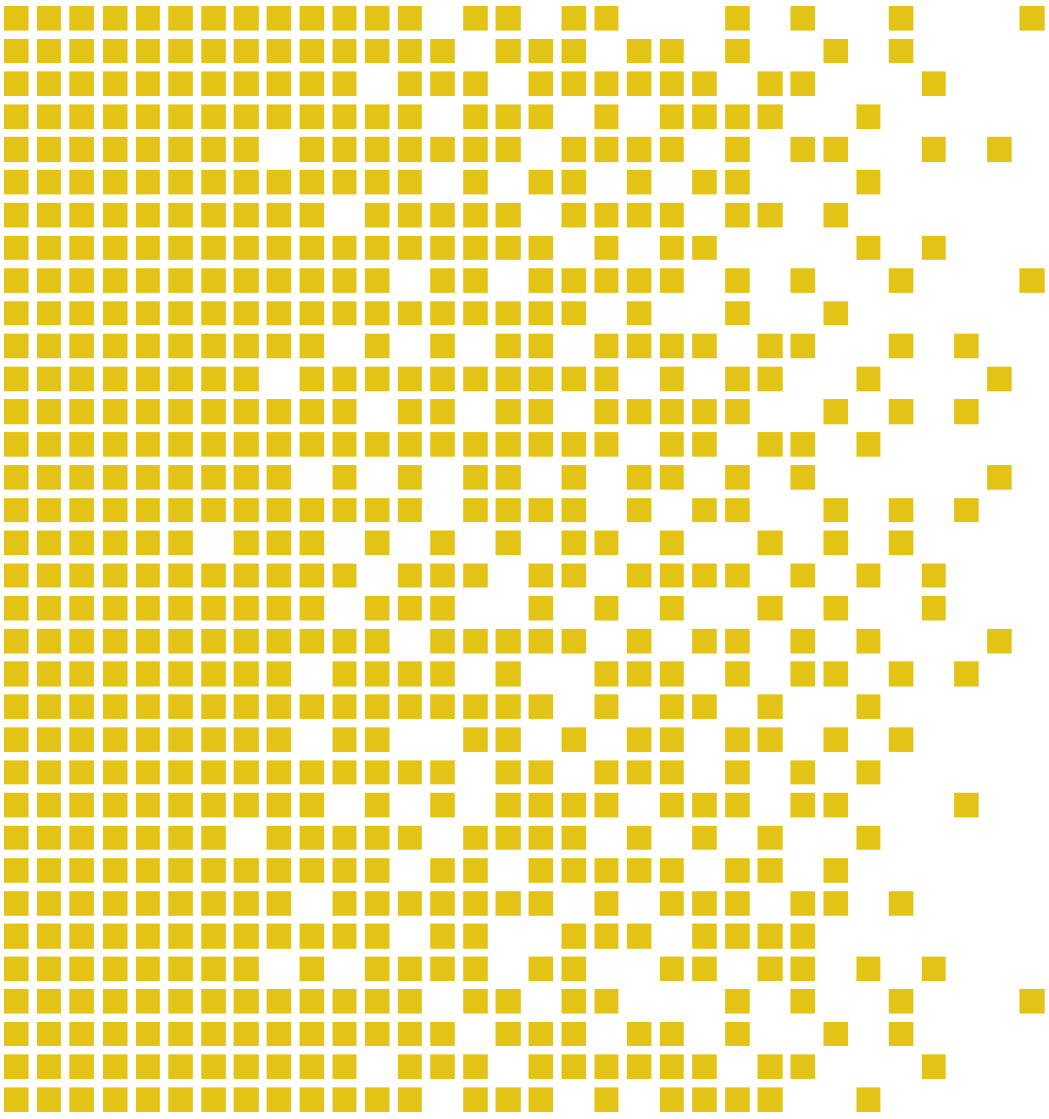
SERTIT-027 CR Certification Report

Issue 1.0 21 December 2010

Toshiba T6ND5 HW version 5



SERTIT, P.O. Box 14, N-1306 Bærum postterminal, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party. [*]

[* Mutual Recognition under the CC recognition arrangement applies to EAL 4 but not to AVA_VAN.5 and ALC_DVS.2.]

Contents

1 Certification Statement

TOSHIBA CORPORATION Semiconductors Company T6ND5 Integrated Circuit is a integrated circut with a DES accelerator combined with a IC for communication to realise an electronic purse.

T6ND5 Integrated Circuit version 5 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and have met the Common Criteria Part 3 augmented requirements of Evaluation Assurance Level EAL 4+ (AVA_VAN.5 and ALC_DVS.2) for the specified Common Criteria Part 2 conformant functionality for the specified environment when running on the platforms specified in Annex A.

It has also met the requirements of Protection Profile Security IC Platform Protection Profile, version 1.0.

Author	Kjartan Jæger Kvassnes Certifier
Quality Assurance	Lars Borgos Quality Assurance
Approved	Kjell W. Bergan Head of SERTIT
Date approved	21 December 2010

2 Abbreviations

BGA	Ball Grid Array
CC	Common Criteria for Information Technology Security Evaluation
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
DEMA	Differential Electro-Magnetic Analysis
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
HW	Hardware
OSP	Organisational Security Policy
POC	Point of Contact
QP	Qualified Participant
SEMA	Simple Electro-Magnetic Analysis
SERTIT	Norwegian Certification Authority for IT Security
SFR	Security Function Policy
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[1] Security Target, TOSHIBA CORPORATION Semiconductors Company, T6ND4 Integrated Circuit Security Target, 30 Nov. 2010, Version 0.01.

[2] Common Criteria Part 1, CCMB-2009-07-001, Version 3.1 R3, July 2009.

[3] Common Criteria Part 2, CCMB-2009-07-002, Version 3.1 R3, July 2009.

[4] Common Criteria Part 3, CCMB-2009-07-003, Version 3.1 R3, July 2009.

[5] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2009-07-004, Version 3.1 R3, July 2009.

[7] Evaluation Technical Report Common Criteria EAL4+ Evaluation of Toshiba T6ND4/T6ND5 Integrated Circuit, 20101210 version 1.0

[8] T6ND4 Functional Specification, Version 0.34, 6 July 2010

[9] T6ND4 User guidance overview, version 0.18, 13 October 2010

[10] T6ND4 User Guidance Manual, version 0.94, 10 August 2010

[11] T6ND4 Custmer Specification, Revision 1.0.0, 2010/03/01

[12] T6ND4 Quality Assurance Document, Version 0.17, 29 November 2010

[13] T6ND4 HW Configuration, version 0,97

[14] Security IC Platform Protection Profile. Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035, version 1.0, June 15, 2007

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of T6ND5 Integrated Circuit version 5 to the Sponsor, TOSHIBA CORPORATION Semiconductors Company, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target [1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The version of the product evaluated was T6ND5 Integrated Circuit and version 5.

This product is also described in this report as the Target of Evaluation (TOE). The developer was TOSHIBA CORPORATION Semiconductors Company.

T6ND5 is a package derivative of the certified chip T6ND4. The T6ND5is a 64 pin BGA package.

The T6ND4 Integrated Circuit is an Integrated Circuit (41 pin BGA package) with a DES accelerator. The TOE is a single chip microcontroller (hardware, security IC dedicated software to initialise a number of settings for sensor levels and countermeasures at start-up and security IC dedicated test software) that is used in mobile equipment. The TOE combined with an IC for communication (which is not part of the TOE) realizes a platform for electric purse.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

The TOE scope is described in the ST[1], chapter 1.3

4.4 Protection Profile Conformance

The Security Target[1] claimed conformance to the following protection profile:

Security IC Platform Protection Profile, version 1.0[14]

The Security Target[1] also includes objectives and security functions additional to those of the protection profile. These are described in the ST, chapter 4.1 and 4.2.

4.5 Assurance Level

The Security Target[1] specified the assurance requirements for the evaluation. The assurance incorporated predefined evaluation assurance level EAL 4, augmented by

AVA_VAN.5 and ALC_DVS.2. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

The TOE security policies are detailed in *ST[1] chapter 3.3*

4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats, OSP's which these objectives meet and security functional requirements and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

4.8 Threats Countered by the TOE

- Physical Manipulation
- Physical Probing
- Malfunction due to Environmental Stress
- Inherent Information Leakage
- Forced Information Leakage
- Abuse of Functionality
- Deficiency of Random Numbers

4.9 Threats Countered by the TOE's environment

There are no threats countered by the TOE's environment.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

The assumptions for the TOE are described in the Protection Profile[14], chapter 3.4

4.12 IT Security Objectives

- The TOE shall maintain the integrity of User Data and of the Security IC Embedded Software (when being executed/processed and when being stored in the TOE's memories)
- The TOE shall maintain the confidentiality of User Data and of the Security IC Embedded Software (when being processed and when being stored in the TOE's memories)

- The TOE shall provide true random numbers
- The TOE shall provide the cryptographic functionality to calculate a DES encryption and decryption to the security IC embedded software

4.13 Non-IT Security Objectives

Security objectives for the development environment

- Usage of Hardware Platform

  The TOE supports cipher schemes as additional specific security functionality. If required the security IC embedded software shall use these cryptographic services of the TOE and their interface as specified.

- Treatment of User Data

  By definition cipher or plain text data and cryptographic keys are User Data. The security IC embedded software shall treat these data appropriately, use only proper secret keys (chosen from a large key space) as input for the cryptographic function of the TOE and use keys and functions appropriately in order to ensure the strength of cryptographic operation.

Security objectives for the operational environment

- Protection during composite product manufacturing

  Security procedures shall be used after TOE Delivery from manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

4.14 Security Functional Requirements

The TOE provides security functions to satisfy the following Security Functional Requirements (SFRs):

- Limited fault tolerance FRU_FLT.2
- Failure with preservation of secure state FPT_FLS.1
- Limited capabilities FMT_LIM.1
- Limited availability FMT_LIM.2
- Audit storage FAU_SAS.1
- Resistance to physical attack FPT_PHP.3
- Basic internal transfer protection FDP_ITT.1
- Subset information flow control FDP_IFC.1
- Basic internal TSF data transfer protection FPT_ITT.1

- Quality metric for random numbers FCS_RNG.1
- Cryptographic operation FCS_COP.1
- Import of user data without security attributes FDP_ITC.1
- Cryptographic key generation FCS_CKM.1
- Cryptographic key destruction FCS_CKM.4
- Secure security attributes FMT_MSA.2

4.15 Security Function Policy

User Data and TSF data shall not be accessible from the TOE except when the Security IC Embedded Software decides to communicate the User Data via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the Security IC Embedded Software.

4.16 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[6].

SERTIT monitored the evaluation which was carried out by the Brightsight B.V. Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR)[7] to SERTIT on the 10. December 2010. SERTIT then produced this Certification Report.

4.17 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities

have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3 [4]. These classes comprise the EAL 4 assurance package augmented with AVA_VAN.5 and ALC_DVS.2.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_VAN.5	Advanced methodical vulnerability analysis

All assurance classes were found to be satisfactory and were awarded an overall "pass" verdict.

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[7] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

Delivery procedures for the TOE are described in the supporting documents[9][12].

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been comprised in delivery.

5.3 Installation and Guidance Documentation

Installation procedures are described in detail in the supporting documents[9][10].

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. Developers should follow the guidance[9][10][11] for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

5.5 Vulnerability Analysis

The vulnerability analysis comprised the following steps:

1. The combined set of well-known attacks from the "JIL Attack Methods for Smartcards and Similar Devices" is considered, leading to the list of 11 major attack methods to consider.
2. A theoretical analysis of the TOE type considers all 11 major attack methods against the SFRs clustered in 6 groups, being the 5 from the PP (Malfunctions, Abuse of functionality, Physical Manipulation, Leakage and Random numbers) and 1 extension (Cryptography(DES)). In total 11*6=66 SFR/attack-combinations are possible. The theoretical analysis leads to the exclusion of 31 SFR/attack-combinations as not applicable for this type of TOE.
3. Potential vulnerabilities from the other evaluation activities have been gathered and taken into account during the analysis. The potential

vulnerabilities in the other IRs indicated that light manipulation should be considered in the perturbation penetration testing.

4. An analysis based on design information analysing SFR/attack-combinations, showing which combinations are not applicable or not possible on this particular TOE, or which need further penetration testing. For 32 of the SFR/attack-combinations sufficient assurance could be found in the design information and other evaluation activities. For 3 SFR/attack-combinations further penetration testing was deemed necessary: for light injection on the FPT_FLS.1/FRU_FLT.2 SFRs, and DEMA on DES for the FDP_ITT.1/FPT_ITT.1/FDP_IFC.1 SFRs.

The TSF is resistant against known attacks at the given time of evaluation, but this could change in the future as attack techniques become more sophisticated.

5.6 Developer's Tests

The testing results from the developer show that the TOE exhibits the expected behaviour at TSFI and SFR enforcing module level. The developers test specification are directly linked to its corresponding functional specification, and passing one test shows that that specific functional specification works according to the documentation.

The depth and coverage analysis shows that the developers' tests cover all TSF, and that the TOE has been extensively tested against its functional specification. The developer's testing results lead either to a test is passed, or the test is failed and an error report is created for that error.

The results show that the developer testing requirements are extensive and that the TSF satisfies the TOE security functional requirements.

5.7 Evaluators' Tests

For independent testing, the evaluator has chosen to perform some additional testing although the developer's testing was extensive but some additional assurance could be gained by additional testing.

The evaluator's independent testing was spread over nearly all interfaces involved for implementation of the SFRs to provide good rigour of testing. Summarized, this testing covers the interfaces involved in the implementation of the SFRs, with some exceptions

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that T6ND5 Integrated Circuit version 5 [running on platforms] meet the specified Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 4+ (AVA_VAN.5 and ALC_DVS.2) for the specified Common Criteria Part 2 conformant functionality and the Protection Profile Security IC Platform Protection Profile, version 1.0, in the specified environment.

6.2 Recommendations

Prospective consumers of T6ND5 Integrated Circuit version 5 should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be used. This is specified in Annex A.

Annex A: Evaluated Configuration

TOE Identification

The T6ND4 Integrated Circuit is an Integrated Circuit (41 pin BGA package) with a DES accelerator. The TOE is a single chip microcontroller that is used in mobile equipment. The TOE combined with an IC for communication realizes a platform for electric purse. The TOE has three different communication interfaces:

- an interface, a wireless interface that receives modulation data from the IC for communication
- a mobile host interface, a wired serial interface that communicates with the host controller of the mobile equipment
- a RFChip interface, a local serial bus that monitors the IC for communication

The objective of the TOE is to protect the IT security of the IC and embedded software that is intended to be used as an electronic purse.

The T6ND4 TOE has been designed to realize card functionality in combination with an RF LSI chip (I-chip) for an electronic purse function (e.g electronic payment) in devices as mobile phone etc. Operating like this there can be a user OS in the ROM and service data in the EEPROM. For example, a commuter ticket, electronic money or data are stored in the EEPROM. The data the I-chip receives is communicated to the TOE by wireless communication. The TOE manages the data securely, and returns the processed result through I-chip to the Reader/writer (R/W).

TOE Documentation

The supporting guidance documents evaluated were:

[a] T6ND4 User guidance overview, version 0.18

[b] T6ND4 Customer specification, version 1.00

[c] T6ND4 User Guidance manual, version 0,94

[d] T6ND4 HW Configuration, version 0,97

Further discussion of the supporting guidance material is given in Section 5.3 "Installation and Guidance Documentation".

TOE Configuration

The following configuration was used for testing:

Item	Identifier	Version
Hardware	T6ND4 Integrated Circuit	5.0
Software	Hardware configuration (CODE)	0.97
	Hardware configuration (Data)	0.97
	TEST ROM software	0.02